LERMAN SENTER PLLC

WASHINGTON, DC

STEPHEN E. CORAN
202.416.6744
SCORAN@LERMANSENTER.COM

October 6, 2016

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: **Protecting the Privacy of Customers of Broadband and Other Telecommunications Services**
WC Docket No. 16-106
Notice of Ex Parte Presentation

Dear Ms. Dortch:

On October 4, 2016, Alex Phillips, President of Rural Broadband Network Services and President of the Wireless Internet Service Providers Association ("WISPA"), S. Jenell Trigg and Deborah J. Salons of Lerman Senter PLLC, and the undersigned, representing WISPA, met with Daniel Kahn, Lisa Hone, Melissa Kirkel, Sherwin Siy, David Brody and Brian Hurley (via telephone) of the Wireline Competition Bureau ("Bureau") to discuss the rules proposed in the *NPRM* in the above-referenced proceeding for protecting the privacy of customers of broadband and other telecommunication services.[1]

The WISPA representatives highlighted issues consistent with WISPA's Comments[2] and Reply Comments[3] submitted in the above-referenced proceeding. The WISPA representatives emphasized the burdens enhanced privacy regulations will have on small broadband providers and the consumers they serve. We expressed support for a small business exemption or, in the alternative, delayed compliance implementation dates based on size tiers in which the providers with the smallest number of customers would have the longest time to comply with whatever rules the Commission adopts. The WISPA representatives further explained that the proposed rules cannot be looked at in a vacuum, as small providers are or may be subject to a "grand slam"

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, 31 FCC Rcd 2500 (rel. April 1, 2016) ("*NPRM*").
[2] Comments of WISPA, WC Docket No. 16-106 (filed May 27, 2016) ("WISPA Comments").
[3] Reply Comments and Additional Comments on the Initial Regulatory Flexibility Analysis of WISPA, WC Docket No. 16-106 (filed July 6, 2016) ("WISPA Reply Comments").

of regulations: Title II regulation, enhanced transparency rules, outage reporting requirements and the proposed privacy rules.

The WISPA representatives expressed support for adoption of rules based on the Federal Trade Commission's approach and an opt-out regime for non-sensitive personally identifiable information. WISPA expressed concern that the information categorized as sensitive would be over-inclusive. We also expressed concern regarding what may constitute a "material" change to a privacy policy that would trigger notice requirements and suggested that the Commission adopt a definition of "material" that considers the effect of a privacy policy change on the rights and obligations of existing customer. We explained that it is possible to make substantial changes to a privacy policy when adding new features or services, without changing an existing customer's opt-in or opt-out rights, or the collection, use or disclosure of a customer's Customer Proprietary Information. In addition, the WISPA representatives expressed their support for the adoption of a privacy policy safe harbor that could be developed by the FCC's Consumer Advisory Committee ("CAC").

The WISPA representatives explained that the proposed seven-day data breach notification requirement to the FCC was too short, and stated that at seven days many providers do not have all of the facts to report. The WISPA representatives also explained that proposed Section 64.7005(b) of the rules should include language that requires the Commission to consider the provider's size in determining whether its data security measures are "reasonably implemented."

Ms. Trigg also conducted a follow-up telephone call with Ms. Hone on Wednesday, October 5, pertaining to the proposed security breach notification requirements under Sec. 64.7006(a)(2)(v) and the "reasonable risk of harm" trigger now under consideration by the Bureau. In particular, Ms. Trigg inquired whether the proposed requirement for information to consumers about national credit-reporting agencies would be necessary for breaches that did not implicate financial harm such as credit card fraud, or fraudulent loans. She explained that WISPA's concern is that the inclusion of such credit-reporting agency information could be unnecessarily alarming and confusing to consumers that would not need such reporting if the breach was of an email without any other identifying information or a password or user ID, or another form of Customer Proprietary Information that would not cause a risk of financial harm. While an unauthorized acquisition of only an email address could be used for spearfishing (a form of ID theft), it is not clear how spearfishing would implicate a consumer's credit report, or whether Equifax, TransUnion, or Experian's various credit monitoring services would address any perceived or potential problem for other types of harm, e.g. reputational harm. Unlike the standard breach notifications required under various state security breach notification laws that are for breaches of sensitive information such as SSN, driver's license numbers, financial accounts, and health information, the Commission's broad scope of Customer Proprietary

Information (sensitive and non-sensitive) subject to notification is much broader than pertinent state laws. WISPA respectfully requests that the Commission consider flexibility for the BIAS provider to provide information to a consumer regarding a credit-reporting agency be based on the scope and nature of the breach, and type of harm at risk.

Pursuant to Section 1.1206 of the Commission's Rules, this letter is being filed electronically via the Electronic Comment Filing System in the above-captioned proceeding.

Respectfully submitted,

/s/ Stephen E. Coran
Stephen E. Coran

cc: Daniel Kahn
Lisa Hone
Melissa Kirkel
Sherwin Siy
David Brody
Brian Hurley